Industrial Control Systems

ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

TLP: White

Analysis of the Cyber Attack on the Ukrainian Power Grid

Defense Use Case

March 18, 2016

1325 G Street NW
Suite 600
Washington, DC 20005
404-446-9780 #2 | www.eisac.com

Table of Contents

Preface

Analysis of the Cyber Attack on the Ukrainian Power Grid

This is an analysis by a joint team to provide a lessons learned community resource from the cyber attack on the Ukrainian power grid. The document is being released as Traffic Light Protocol: White (TLP: White) and may be distributed without restriction, subject to copyright controls. This document, the Defense Use Case (DUC), summarizes important learning points and presents several mitigation ideas based on publicly available information on ICS incidents in Ukraine. The E-ISAC and SANS are providing a summary of the available information compiled from multiple publicly available sources as well as analysis performed by the SANS team in relation to this event.[1] This document provides specific mitigation concepts for power system Supervisory Control and Data Acquisition (SCADA) defense, as well as a general learning opportunity for ICS defenders.

Authors, working with the E-ISAC:
Robert M. Lee, SANS
Michael J. Assante, SANS
Tim Conway, SANS

[1] The SANS investigation into this incident should not be confused with the U.S. interagency team investigation or any other organization or company's efforts to include the E-ISAC's past reporting. SANS ICS team has been analyzing the data on their own since December 25, 2015, and has provided its analysis to the wider community. This document is provided to E-ISAC and the North American electricity sector to benefit its members and the larger critical infrastructure community.

Summary of Incidents

On December 23, 2015, the Ukrainian Kyivoblenergo, a regional electricity distribution company, reported service outages to customers. The outages were due to a third party's illegal entry into the company's computer and SCADA systems: Starting at approximately 3:35 p.m. local time, seven 110 kV and 23 35 kV substations were disconnected for three hours. Later statements indicated that the cyber attack impacted additional portions of the distribution grid and forced operators to switch to manual mode.[2, 3] The event was elaborated on by the Ukrainian news media, who conducted interviews and determined that a foreign attacker remotely controlled the SCADA distribution management system.[4] The outages were originally thought to have affected approximately 80,000 customers, based on the Kyivoblenergo's update to customers. However, later it was revealed that three different distribution oblenergos (a term used to describe an energy company) were attacked, resulting in several outages that caused approximately 225,000 customers to lose power across various areas.[5, 6]

Shortly after the attack, Ukrainian government officials claimed the outages were caused by a cyber attack, and that Russian security services were responsible for the incidents.[7] Following these claims, investigators in Ukraine, as well as private companies and the U.S. government, performed analysis and offered assistance to determine the root cause of the outage.[8] Both the E-ISAC and SANS ICS team was involved in various efforts and analyses in relation to this case since December 25, 2015, working with trusted members and organizations in the community.

This joint report consolidates the open source information, clarifying important details surrounding the attack, offering lessons learned, and recommending approaches to help the ICS community repel similar attacks. This report does not focus on attribution of the attack.

[2] https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid
[3] http://news.finance.ua/ua/news/-/366136/hakery-atakuvaly-prykarpattyaoblenergo-znestrumyvshy-polovynu-regionu-na-6-godyn
[4] http://ru.tsn.ua/ukrayina/iz-za-hakerskoy-ataki-obestochilo-polovinu-ivano-frankovskoy-oblasti-550406.html
[5] http://www.oe.if.ua/showarticle.php?id=3413
[6] https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01
[7] http://www.ukrinform.net/rubric-crime/1937899-russian-hackers-plan-energy-subversion-in-ukraine.html
[8] https://www.rbc.ua/rus/news/pravitelstva-ssha-ukrainy-rassmotryat-otchet-1454113214.html

Summary of Information and Reporting

Background

On December 24, 2015, TSN (a Ukrainian news outlet) released the report "Due to a Hacker Attack Half of the Ivano-Frankivsk Region is De-Energized."[9] Numerous reporting agencies and independent bloggers from the Washington Post, SANS Institute, New York Times, ARS Technica, BBC, Wired, CNN, Fox News, and the E-ISAC Report have followed up on the initial TSN report.[10] These subsequent reports have collectively provided details of a cyber attack that targeted the Ukrainian electric system. The U.S. Department of Homeland Security (DHS) issued a formal report on February 25, 2016, titled IR-ALERT-H-16-056-01.[11] Based on the DHS report, three Ukrainian oblenergos experienced coordinated cyber attacks that were executed within 30 minutes of each other. The attack impacted 225,000 customers and required the oblenergos to move to manual operations in response to the attack.

The oblenergos were reportedly able to restore service quickly after an outage window lasting several hours.[12] The DHS report states that, while electrical service was restored, the impacted oblenergos continue to operate their distribution systems in an operationally constrained mode. Within the Ukrainian electrical system, these attacks were directed at the regional distribution level, as shown in Figure 1.

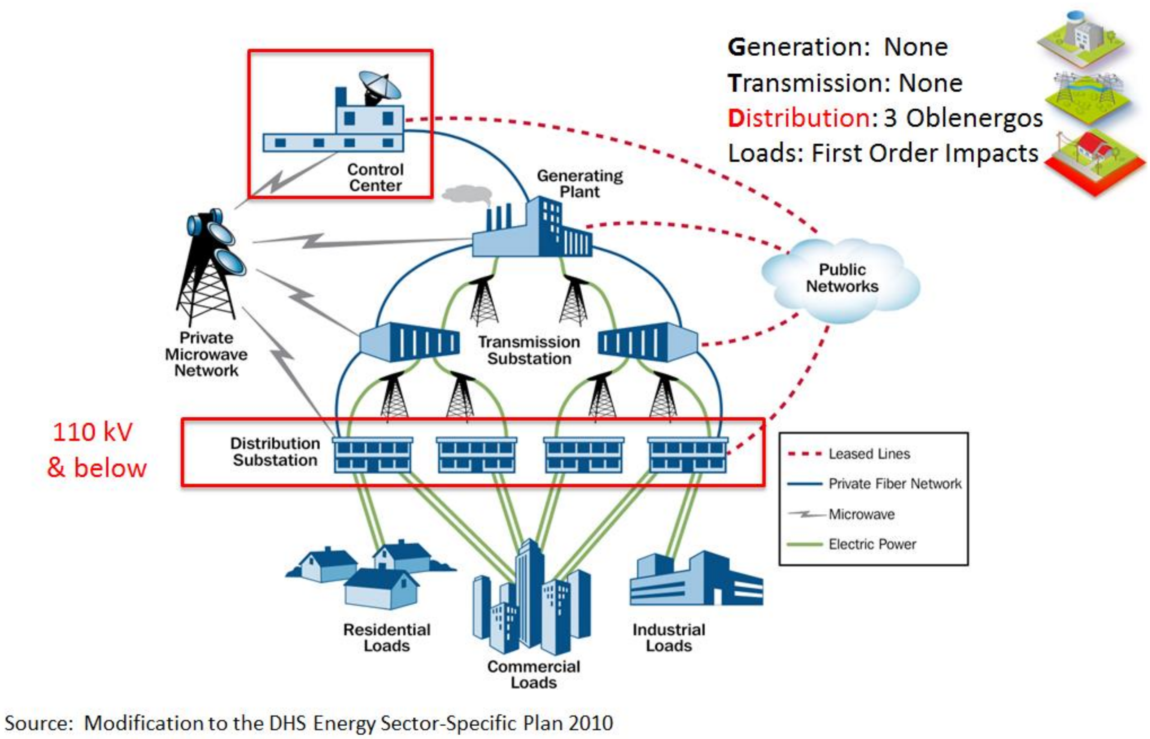


Figure 1: Electric System Overview

[9] http://ru.tsn.ua/ukrayina/iz-za-hakerskoy-ataki-obestochilo-polovinu-ivano-frankovskoy-oblasti-550406.html

[10] E-ISAC: Mitigating Adversarial Manipulation of Industrial Control Systems as Evidenced by Recent International Events, February 9, 2016 (TLP=RED)

11 https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

12 https://www.washingtonpost.com/world/national-security/russian-hackers-suspected-in-attack-that-blacked-out-parts-of-ukraine/2016/01/05/4056a4dc-b3de-11e5-a842-0feb51d1d124_story.html

See the Appendix for an evaluation of the credibility and amount of technical information that is publicly available.

Keeping Perspective

The cyber attacks in Ukraine are the first publicly acknowledged incidents to result in power outages. As future attacks may occur, it is important to scope the impacts of the incident. Power outages should be measured in scale (number of customers and amount of electricity infrastructure involved) and in duration to full restoration. The Ukrainian incidents affected up to 225,000 customers in three different distribution-level service territories and lasted for several hours. These incidents should be rated on a macro scale as low in terms of power system impacts as the outage affected a very small number of overall power consumers in Ukraine and the duration was limited. In contrast, it is likely that the impacted companies rate these incidents as high or critical to the reliability of their systems and business operations.

Attacker Tactics Techniques and Procedures Description

Direct attribution is unnecessary to learn from this attack and to consider mitigation strategies; it is only necessary to use the mental model of how the cyber actor works to understand the capabilities and general profile against which one is defending. The motive and sophistication of this power grid attack is consistent with a highly structured and resourced actor. This actor was co-adaptive and demonstrated varying tactics and techniques to match the defenses and environment of the three impacted targets. The mitigation section of this document provides mitigation concepts related to the attack and how to develop a more lasting mitigation strategy by anticipating future attacks.

Capability

The attackers demonstrated a variety of capabilities, including spear phishing emails, variants of the BlackEnergy 3 malware, and the manipulation of Microsoft Office documents that contained the malware to gain a foothold into the Information Technology (IT) networks of the electricity companies.[13] They demonstrated the capability to gain a foothold and harvest credentials and information to gain access to the ICS network. Additionally, the attackers showed expertise, not only in network connected infrastructure; such as Uninterruptable Power Supplies (UPSs), but also in operating the ICSs through supervisory control system; such as the Human Machine Interface (HMI), as shown in Figure 2.

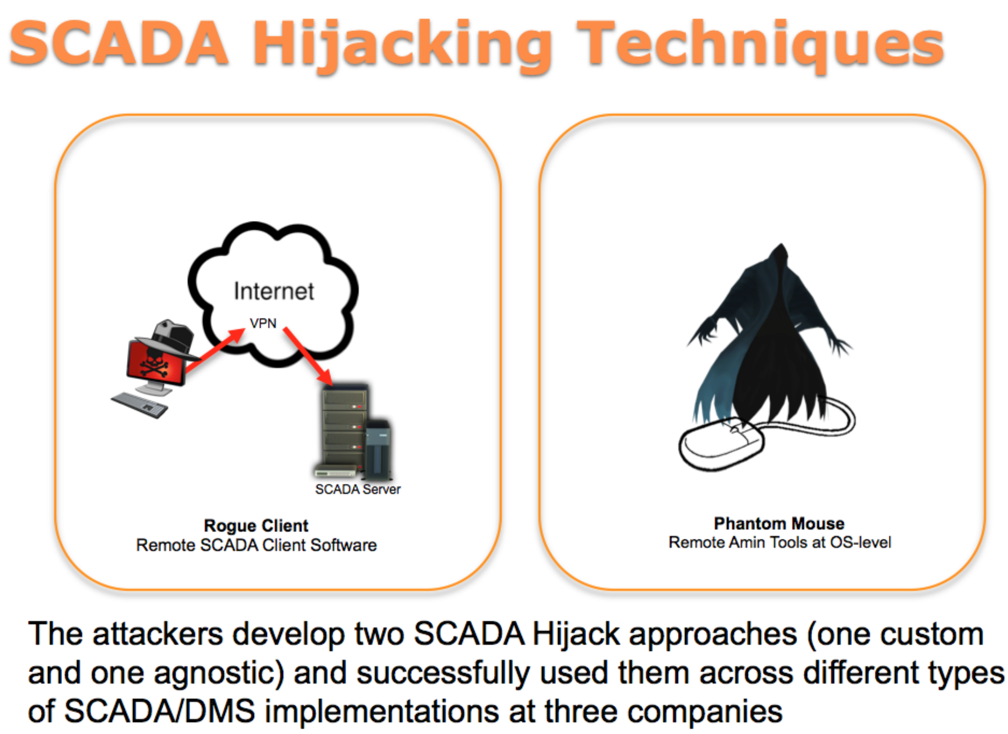


Figure 2: Control & Operate: SCADA Hijacking Techniques

Finally, the adversaries demonstrated the capability and willingness to target field devices at substations, write custom malicious firmware, and render the devices, such as serial-to-ethernet convertors, inoperable and

[13] For a discussion around the history of the BlackEnergy 3 malware and Sandworm team see the SANS ICS webcast with iSight here: https://www.sans.org/webcasts/analysis-sandworm-team-ukraine-101597

unrecoverable.[14] In one case, the attackers also used telephone systems to generate thousands of calls to the energy company's call center to deny access to customers reporting outages. However, the strongest capability of the attackers was not in their choice of tools or in their expertise, but in their capability to perform long-term reconnaissance operations required to learn the environment and execute a highly synchronized, multistage, multisite attack.

The following is a consolidated list of the technical components used by the attackers, graphically depicted in Figure 3:

- Spear phishing to gain access to the business networks of the oblenergos
- Identification of BlackEnergy 3 at each of the impacted oblenergos
- Theft of credentials from the business networks
- The use of virtual private networks (VPNs) to enter the ICS network
- The use of existing remote access tools within the environment or issuing commands directly from a remote station similar to an operator HMI
- Serial-to-ethernet communications devices impacted at a firmware level[15]
- The use of a modified KillDisk to erase the master boot record of impacted organization systems as well as the targeted deletion of some logs[16]
- Utilizing UPS systems to impact connected load with a scheduled service outage
- Telephone denial-of-service attack on the call center

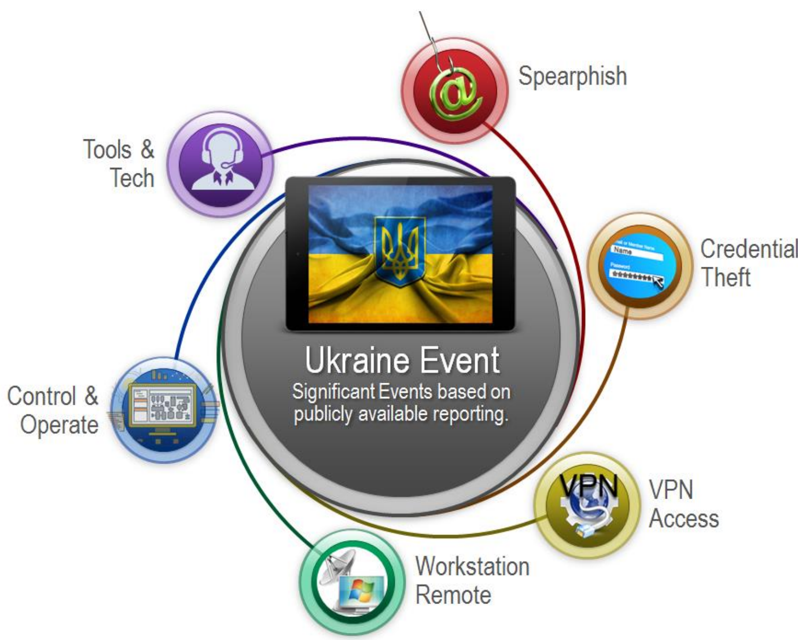


Figure 3: Ukraine Attack Consolidated Technical Components

At various points in the public reporting on the attack, organizations have indicated that BlackEnergy 3 and KillDisk itself could be directly responsible for the outage. One of the items specifically highlighted to support

[14] http://mpe.kmu.gov.ua/minugol/control/uk/publish/article;jsessionid=CE1C739AA046FF6BA00FE8E8A4D857F3.app1?art_id=245086886&cat_id=35109

[15] To learn about serial to ethernet converters and the types of vulnerabilities that exist to them see DigitalBond's Basecamp report here: https://www.digitalbond.com/blog/2015/10/30/basecamp-for-serial-converters/

[16] http://www.symantec.com/connect/blogs/destructive-disakil-malware-linked-ukraine-power-outages-also-used-against-media-organizations

this theory was that KillDisk deleted a process on Windows systems linked to serial-to-ethernet communications.[17] Regardless of the impact of the SCADA network environment, neither BlackEnergy 3 nor KillDisk contained the required components to cause the outage. The outages were caused by the use of the control systems and their software through direct interaction by the adversary. All other tools and technology, such as BlackEnergy 3 and KillDisk, were used to enable the attack or delay restoration efforts.

Opportunities

Multiple opportunities existed for the adversary to execute its attack. External to the oblenergos and prior to the attack, there was a variety of open-source information available; including a detailed list of types of infrastructure such as Remote Terminal Unit (RTU) vendors and versions posted online by ICS vendors.[18] The VPNs into the ICS from the business network appear to lack two-factor authentication. Additionally, the firewall allowed the adversary to remote admin out of the environment by utilizing a remote access capability native to the systems. In addition, based on media reporting, there did not appear to be any resident capability to continually monitor the ICS network and search for abnormalities and threats through active defense measures; like network security monitoring. These vulnerabilities would have provided the adversary the opportunity to persist within the environment for six months or more to conduct reconnaissance on the environment and subsequently execute the attack.[19]

Based on the details provided in the DHS report, the adversary used a consistent attack approach on all three impacted targets. The adversary also used consistent tactics to impact field controllable elements and irreparably damage field devices.

Why these oblenergos were targeted remains an open debate. Based on the public reporting, it is unknown if the targets were selected based on common technologies in use, system architectures, reconnaissance operations, or service territories. Opportunity-based considerations for selecting a specific target may focus on an attacker's confidence and ability to cause an ICS effect. Some example decision factors could include:

- Targets with common systems and configurations
- Multiple systems with common centralized control points
- ICS impact duration estimates (e.g., long term or short term)
- Existing capabilities required to achieve desired results
- Risk level of performing the operation and being discovered
- Achieved access and ability to move and act within the environment

[17] http://www.eset.com/int/about/press/articles/malware/article/eset-finds-connection-between-cyber-espionage-and-electricity-outage-in-ukraine/
[18] http://galcomcomp.com/index.php/ru/nashi-proekty/15-proekt3-material-ru
[19] http://mobile.reuters.com/article/idUSKCN0VL18E

ICS Cyber Kill Chain Mapping

The ICS Cyber Kill Chain was published by SANS in 2015 by Michael Assante and Robert M. Lee as an adaptation of the traditional cyber kill chain developed by Lockheed Martin analysts as it applied to ICSs.[20] The ICS Cyber Kill Chain details the steps an adversary must follow to perform a high-confidence attack on the ICS process and/or cause physical damage to equipment in a predictable and controllable way, as displayed in Figure 4.

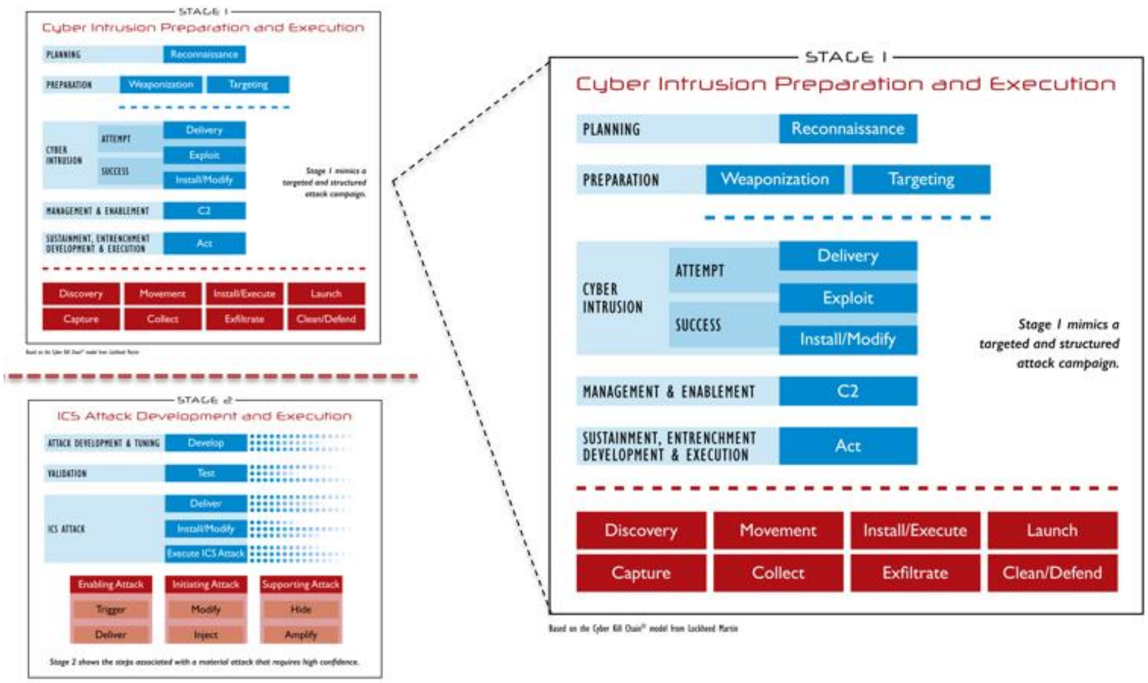


Figure 4: The ICS Cyber Kill Chain with Stage 1 Highlighted

The attack on the Ukrainian power grid followed the ICS Cyber Kill Chain completely throughout Stage 1 and Stage 2. The attack gained access to each level of the ICS, as shown in Figure 5, with the ICS Cyber Kill Chain plotted alongside a segmentation/hierarchy model (e.g., modified Purdue Model). Completing Stage 1 entails a successful cyber intrusion or breach into an ICS system, but is not characterized as an ICS attack. Completion of Stage 2 completed the ICS Kill Chain, resulting in a successful cyber attack that led to an impact on the operations of the ICS. The next section includes a discussion of the two stages using currently available information from the attack.

[20] https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

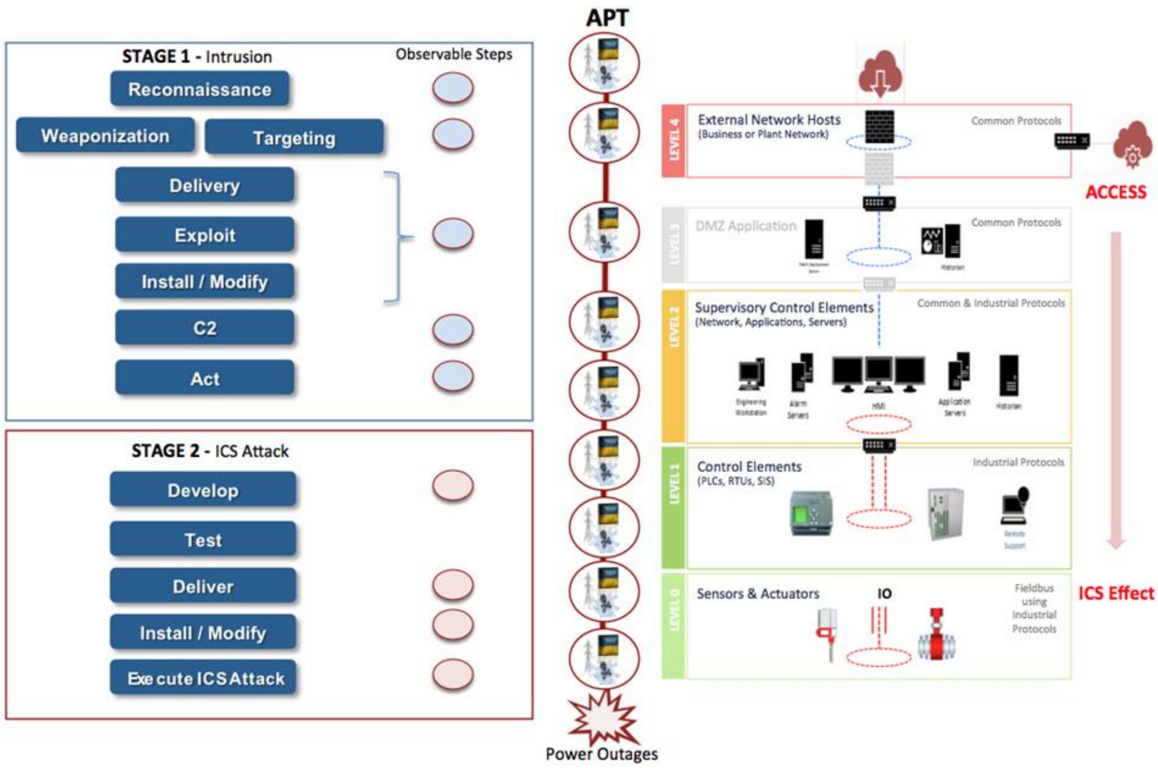


Figure 5: Ukraine Cyber Attack ICS Cyber Kill Chain and Purdue Model Mapping[21]

ICS Cyber Kill Chain Mapping – Stage 1

The first step in Stage 1 is **Reconnaissance**. There were no reports of observed reconnaissance having taken place prior to targeting the energy companies. However, an analysis of the three impacted organizations shows they were particularly interesting targets due to the levels of automation in their distribution system; enabling the remote opening of breakers in a number of substations. Additionally, the targeting and final attack plan for the electricity companies in general were highly coordinated, which indicates that reconnaissance took place at some point. This was very unlikely to have been an opportunistic attack.

The second step is **Weaponization** and/or **Targeting**. Targeting would normally take place when no weaponization is needed; such as directly accessing internet connected devices. In this attack, it does not appear that targeting of specific infrastructure was necessary to gain access. Instead, the adversaries weaponized Microsoft Office documents (Excel and Word) by embedding BlackEnergy 3 within the documents.[22] Samples of Excel and other office documents have been recovered from the broader access campaign that targeted a multitude of organizations in Ukraine; including Office documents used in the specific attack against the three electricity companies.[23, 24]

During the cyber intrusion stage of **Delivery**, **Exploit**, and **Install,** the malicious Office documents were **delivered**

[21] Note, the exact architectures of the impacted utilities are not represented in the figure. The Purdue Model is a standard way of viewing different zones of a well-constructed ICS.

[22] https://securelist.com/blog/research/73440/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/

[23] https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B

[24] Those looking for Indicators of Compromise for the word document, command and control servers, and the malware should look to E-ISAC, ICS-CERT, and iSight private reporting as well as public reporting from Kaspersky Labs, ESET, and CYS Centrum reference: https://cys-centrum.com/ru/news/black_energy_2_3 and https://securelist.com/blog/research/73440/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/

via email to individuals in the administrative or IT network of the electricity companies. When these documents were opened, a popup was displayed to users to encourage them to enable the macros in the document as shown in Figure 6.[25] Enabling the macros allowed the malware to **Exploit** Office macro functionality to install BlackEnergy 3 on the victim system and was not an exploit of a vulnerability through exploit code. There was no observed exploit code in this incident. The theme of using available functionality in the system was present throughout the adversary's kill chain.

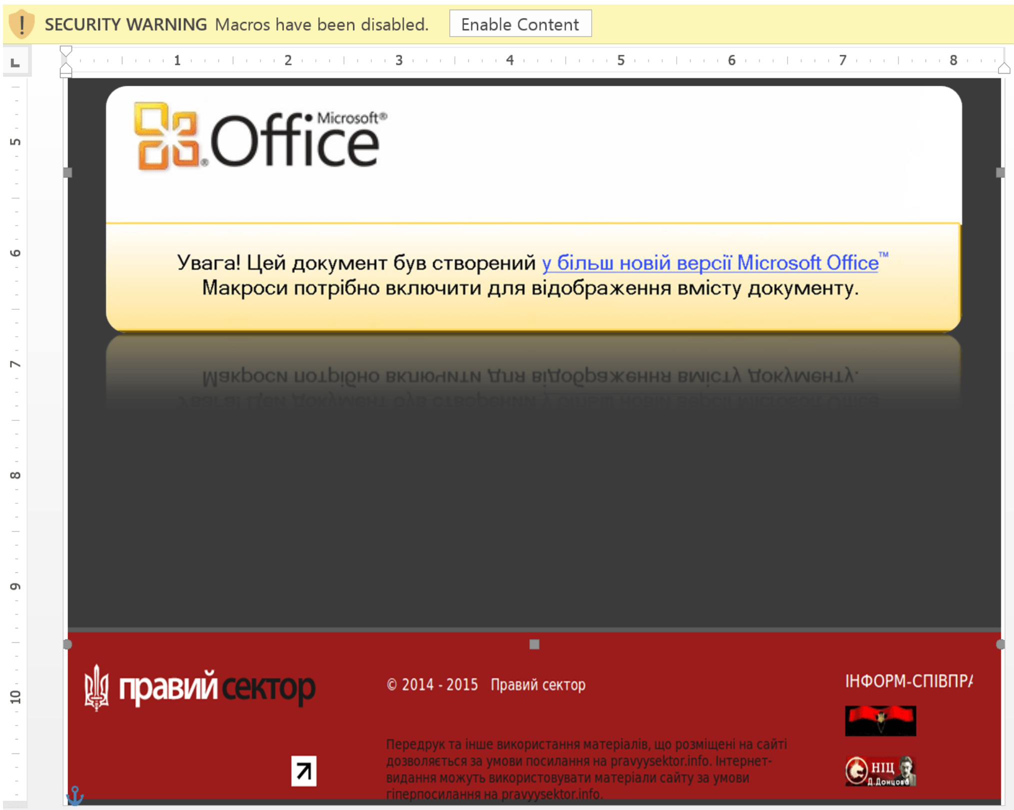


Figure 6: A Sample of a BlackEnergy 3 Infected Microsoft Office Document[26]

Upon the **Install** step, the BlackEnergy 3 malware connected to command and control (C2) IP addresses to enable communication by the adversary with the malware and the infected systems. These pathways allowed the adversary to gather information from the environment and enable access. The attackers appear to have gained access more than six months prior to December 23, 2015, when the power outage occurred.[27] One of their first actions happened when the network was to harvest credentials, escalate privileges, and move laterally throughout the environment (e.g., target directory service infrastructure to directly manipulate and control the authentication and authorization system). At this point, the adversary completed all actions to establish persistent access to the targets. While the initial footholds were used to harvest legitimate credentials for pivoting and systematic takeover of IT systems and remote connections, it is likely that the attackers moved quickly away from their initial footholds and vulnerable C2s in an effort to blend into the target's systems as authorized users. With this information, the attackers would be able to identify VPN connections and avenues from the business network into the ICS network. Using native connections and commands allows the attackers to discover the remainder of the systems and extract data necessary to formulate a plan for Stage 2.

[25] For a detailed understanding of the infected Microsoft Office documents and the malicious payload see Kaspersky Lab's write-up here: https://securelist.com/blog/research/73440/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/

[26] https://securelist.com/blog/research/73440/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/

[27] http://politicalpistachio.blogspot.com/2016/01/russian-hackers-take-down-power-grid-in.html

Speculation

There was not enough publicly available information to determine how diversified the adversary's attack was to include how many different types of devices were impacted at the firmware level. However, through publicly available information about the Ukrainian networks, as well as knowledge of similar electric distribution systems, it is likely that there was a diverse hardware and software environment.

It is suspected that the administrative and ICS networks contained multiple OS versions such as Windows XP and Windows 7, multiple types of RTUs and gateways, and various industrial switches.

Using the stolen credentials, the adversary was able to pivot into the network segments where SCADA dispatch workstations and servers existed. Upon entry into the network, the actions of the adversaries were consistent in theme but different in technical minutia between the three impacted oblenergoss. In at least one of the oblenergos, the attackers discovered a network connected to a UPS and reconfigured it so that when the attacker caused a power outage, it was followed by an event that would also impact the power in the energy company's buildings or data centers/closets.

There is not sufficient information available to identify if any information was exfiltrated from the environment, but the adversary demonstrated a capability in Stage 2 that indicates internal discovery was performed. This reconnaissance would have needed to include discovering field devices such as the serial-to-ethernet devices used to interpret commands from the SCADA network to the substation control systems. Additionally, the three oblenergos used different distribution management systems (DMSs), and the attackers would have needed to perform some network reconnaissance against these systems and find specific targets to execute their highly coordinated attack.[28]

ICS Cyber Kill Chain Mapping – Stage 2

In most cases, the **Develop** stage occurs in the adversary's networks, thereby limiting any available forensic information, but the attack that follows this stage can reveal a lot about the adversarial process. In the Attack Development and Tuning Stage of Stage 2, the attackers executed the Develop step in at least two ways. First, they learned how to interact with the three distinct DMS environments using the native control present in the system and operator screens. Second, and more importantly, they developed malicious firmware for the serial-to-ethernet devices.[29]

Currently available information indicates that the malicious firmware was consistent amongst devices and uploaded within short periods of each other to multiple sites. Therefore, the malicious uploads of firmware was likely developed prior to the attack for quick and predictable execution.

E-ISAC and the SANS ICS team assess with high confidence that, during the Validation Stage of Stage 2, the adversary did **Test** their capabilities prior to their deployment. It is possible that the adversaries were able to execute this with pure luck, but it is highly unlikely and inconsistent with the professionalism observed throughout the rest of the attack. The adversaries likely had systems in their organization that they were able to evaluate and test their firmware against prior to executing on December 23rd.

[28] The three different DMS vendors were discoverable via open-source searching. The names of the vendors are being withheld as it is not important to the discussion of the attack. There were no exploits leveraged against these vendors but they simply abused with direct access.

[29] http://mpe.kmu.gov.ua/minugol/control/uk/publish/article;jsessionid=CE1C739AA046FF6BA00FE8E8A4D857F3.app1?art_id=245086886&cat_id=35109

During the ICS Attack Stage, the adversaries used native software to **Deliver** themselves into the environment for direct interaction with the ICS components. They achieved this using existing remote administration tools on the operator workstations. The threat actors also continued to use the VPN access into the IT environment.[30]

In final preparation for the attack, the adversaries completed the **Install/Modify** stage by installing malicious software identified as a modified or customized KillDisk across the environment. While it is likely the attackers then ensured their modifications to the UPS were ready for the attack, there was not sufficient forensic evidence available to prove this. The last act of modification was for the adversaries to take control of the operator workstations and thereby lock the operators out of their systems. Figure 7 shows the static analysis of the KillDisk API imports following the event.

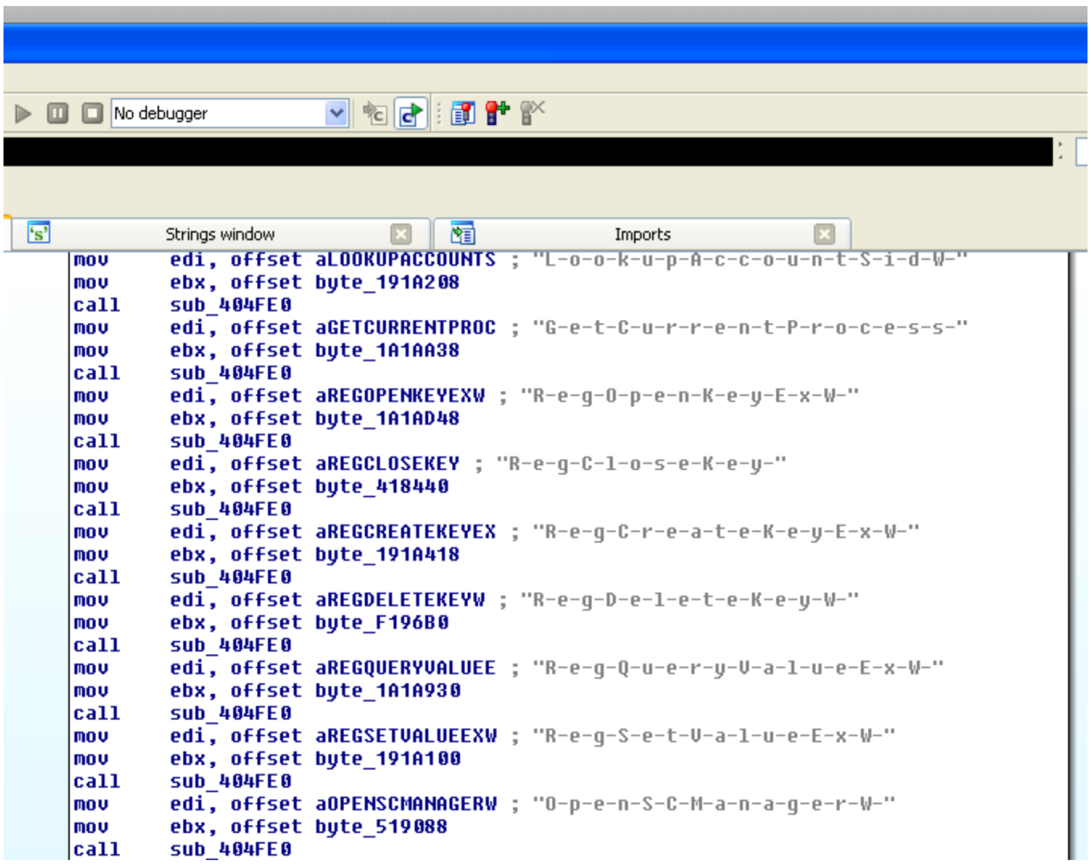


Figure 7: Static Analysis of KillDisk Identifying API Imports[31]

Finally, to complete the ICS Cyber Kill Chain and to **Execute the ICS Attack,** the adversaries used the HMIs in the SCADA environment to open the breakers. At least 27 substations (the total number is probably higher) were taken offline across the three energy companies, impacting roughly 225,000 customers.[32, 33] Simultaneously, the attackers uploaded the malicious firmware to the serial-to-ethernet gateway devices. This ensured that even if

[30] http://mpe.kmu.gov.ua/minugol/control/uk/publish/article;jsessionid=CE1C739AA046FF6BA00FE8E8A4D857F3.app1?art_id=245086886&cat_id=35109

[31] This image was provided by Jake Williams of Rendition InfoSec. It is included here to note that KillDisk would not run properly in a malware sandbox for analysis. Static analysis was required to fully investigate the malware sample.

[32] http://money.cnn.com/2016/01/18/technology/ukraine-hack-russia/

[33] In analysis of the impact observed and on the available information on the Ukrainian distribution grid it is assessed with medium confidence that the public number of disconnected substations, 27, is a low number.

the operator workstations were recovered, remote commands could not be issued to bring the substations back online (We have characterized the firmware attacks against field communication devices as “blowing the bridges”).

During this same period, the attackers also leveraged a remote telephonic denial of service on the energy company’s call center with thousands of calls to ensure that impacted customers could not report outages. Initially, it seemed that this attack was to keep customers from informing the operators of how extensive the outages were; however, in review of the entirety of the evidence, it is more likely that the denial of service was executed to frustrate the customers since they could not contact customer support or gain clarity regarding the outage. The entire attack from March 2015 – December 23, 2015 is graphically depicted below in Figure 8.

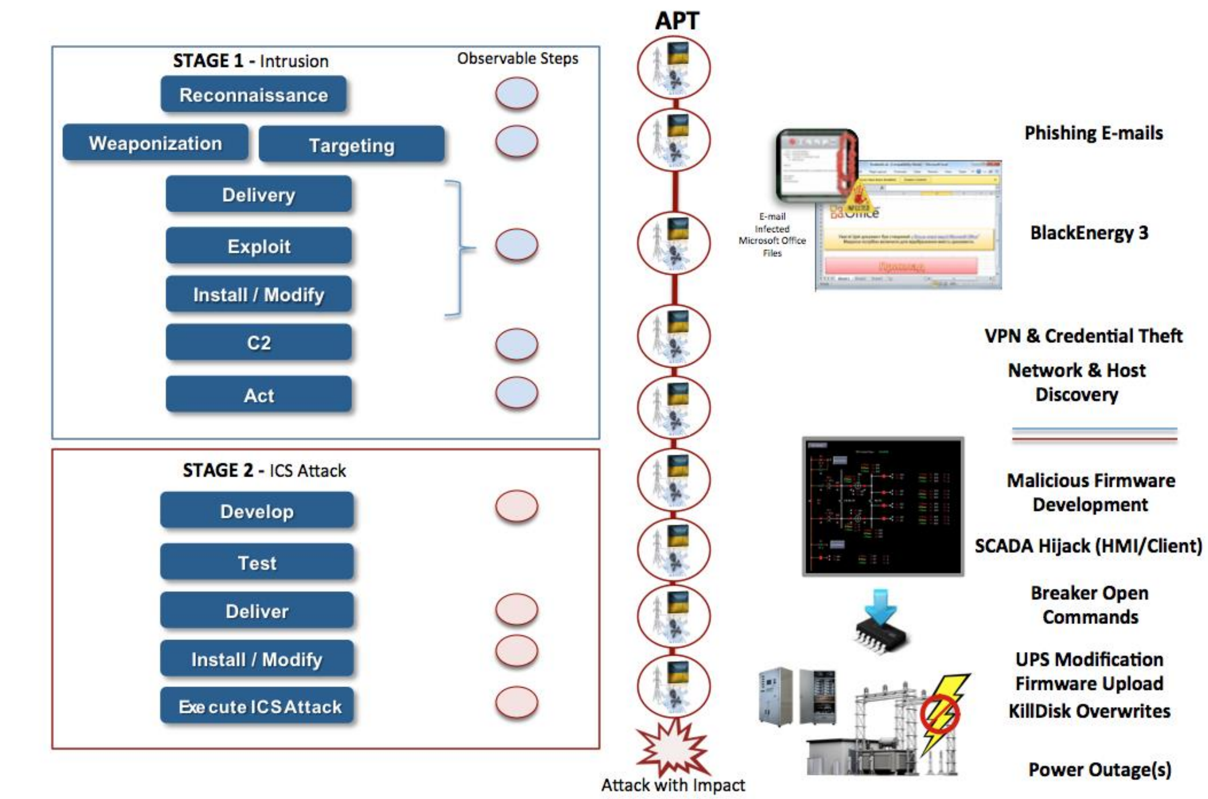


Figure 8: ICS Kill Chain Mapping Chart

It is extremely important to note that neither BlackEnergy 3, unreported backdoors, KillDisk, nor the malicious firmware uploads alone were responsible for the outage. Each was simply a component of the cyber attack for the purposes of access and delay of restoration. For example, on some systems, KillDisk made the Windows systems inoperable by manipulating or deleting the master boot record, but on other systems it just deleted logs and system events.[34, 35] The actual cause of the outage was the manipulation of the ICS itself and the loss of control due to direct interactive operations by the adversary. The loss of view into the system through the wiping of the SCADA network systems simply delayed restoration efforts.

In summary, Stage 2 consisted of the following attack elements:

- **Supporting attacks**:
    - Schedule disconnects for UPS systems
    - Telephonic floods against at least one oblenergos' customer support line
- **Primary attack**: SCADA hijack with malicious operation to open breakers
- **Amplifying attacks**:
    - KillDisk wiping of workstations, servers, and an HMI card inside of an RTU
    - Firmware attacks against Serial-to-Ethernet devices at substations

[34] https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01
[35] https://ics.sans.org/blog/2016/01/01/potential-sample-of-malware-from-the-ukrainian-cyber-attack-uncovered

Defense Lessons Learned – Passive and Active Defenses

We reviewed the mitigation strategies provided through the DHS ICS-CERT Alert and considered how an adversary may alter the next attack based on the mitigation taken by a target. We support many of the mitigation recommendations provided to date. However, it is likely that the adversary will modify attack approaches in follow-on campaigns and these mitigation strategies may not be sufficient. In the following section, we discuss mitigations for the attack that took place to extract defense lessons learned. In addition, we discuss future potential attacker methodologies and provide recommendations that could disrupt similar adversary's operations. The mitigations will focus on recommendations for **Architecture, Passive Defense,** and **Active Defense** methodologies along the Sliding Scale of Cyber Security, shown in Figure 9.[36]

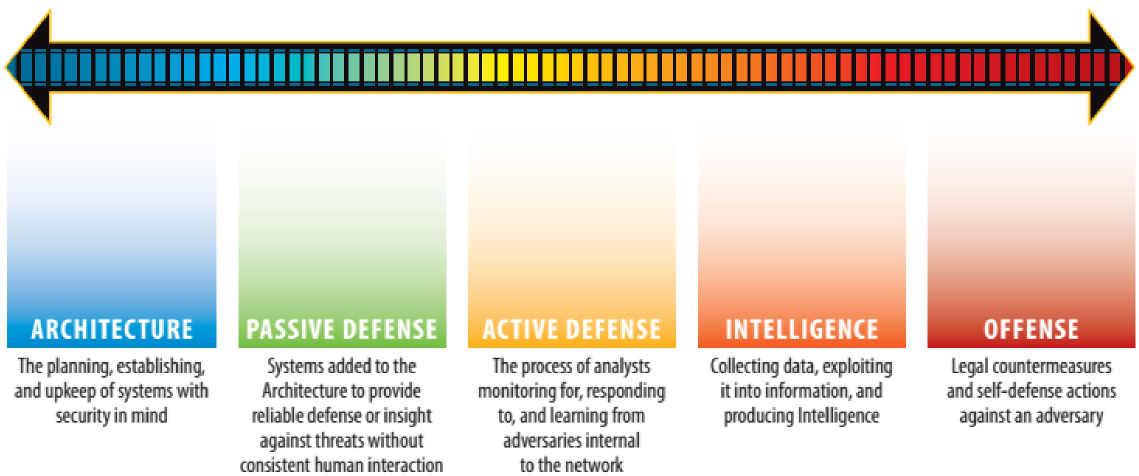


Figure 9: The Sliding Scale of Cyber Security

Spear Phishing

Ukraine Attack

In the attack, the adversary delivered a targeted email with a malicious attachment that appeared to come from a trusted source to specific individuals within the organizations. Initial mitigation recommendations would point to end-user awareness training and ongoing phishing testing. Efforts to prevent malware have often recommended application whitelisting, which can be effective in ICS environments if the ICS vendor approves of the use. However, based on the details of this attack, application whitelisting would have had a limited role contained to the execution of initial dropper infections in network segments with infected workstations (e.g., users that received and activated infected spear phish emails) where application whitelisting may be more challenging to implement. It is important to note that application whitelisting would not have deterred or prevented the second stage ICS attacks that impacted the Ukrainian oblenergos. In at least one instance, the attacker used a remote rogue client and approved OS-level remote admin features for other components of the attack.

The Next Attack

The adversary may conduct follow-on attacks that pursue alternative forms of social engineering campaigns, like targeting the organization through large-scale phishing campaigns, using water-holing attacks, or conducting direct-call campaigns to users or the help desk. They could also leverage technical exploits not requiring social engineering of personnel.

[36] https://www.sans.org/reading-room/whitepapers/analyst/sliding-scale-cyber-security-36240

Opportunities to Disrupt

The adversary will likely modify attacks to respond to increases or changes in the target's defenses. Defenders need to develop anticipatory responses to attack effects. Since the social engineering components of attacks targeted email and internet accessible cyber assets, these assets and the networks they reside on are untrusted contested territory. Communication with these untrusted areas should be segmented, monitored, and controlled. Operate under the assumption that the environment is accessible by the adversary and ensure appropriate defenses are in place to protect the operations and control environment from the adversary-controlled business cyber assets (while some organizations inherently trust their business systems and networks, additional enforcement and scrutiny of these systems is necessary). Consider using sandboxing technology to evaluate documents and emails coming into the network, using proxy systems to control outbound and inbound communication paths, and limiting workstations to communicate only through the proxy devices by implementing perimeter egress access controls.

Credential Theft

Ukraine Attack

In the attack, the adversary appears to have used BlackEnergy 3 to establish a foothold and utilize keystroke loggers to perform credential theft. As an initial mitigation approach, we recommend that organizations obtain the YARA rules for the latest IOCs. By using the YARA forensic tool, organizations can search for BlackEnergy 3 infections and then utilize antimalware removal tools to eliminate the malware from the infected assets. Defenders should be mindful of the time it takes to detect an infected host as the intruder may have already moved inside the network and secured additional methods to interact and communicate with the infected network. Organizations should change user and shared user passwords (ensure that these steps are approved by operations and the vendor, and tested for impacts to operations and existing security controls).

The Next Attack

Adversaries with persistent access will simply use a different remote access Trojan, an updated version of BlackEnergy 3, or an alternate mode of credential attacks. To detect and mitigate adversary movement throughout an environment and account manipulation, mitigation efforts should be focused on directory (e.g., Active Directory, Domain, eDirectory, and LDAP) segmentation with organizational unit trust models. This approach would allow early detection and prevent some basic attacker approaches.

Opportunities to Disrupt

Monitor user account behavior, network and system communication, and directory-level activity with a focus on identifying abnormalities. Implement alarm capabilities with different priority-level alarms based on the risk of the systems associated with the alarms. It is important to note that YARA is a forensics tool and is not a continuous monitoring solution.

Data Exfiltration

Ukraine Attack

After the attackers achieved the necessary freedom of movement and action in the IT infrastructure, they began exfiltrating the necessary information and discovering the hosts and devices to devise an attack concept to hijack the SCADA DMS to open breakers and cause a power outage. They followed this with destructive attacks against workstations, servers, and embedded devices that provide industrial communications in their distribution substations. The mitigation recommendation here is to understand where this type of information exists inside your business network and ICSs. Minimizing where the information resides and controlling access is

a priority for an ICS dependent organization.

The Next Attack

Attackers may look deeper into the ICS configuration and settings or controller and protection/safety logic. Ensure to maintain a vaulted copy of known good project files, control and safety logic, and firmware. Also using file integrity checkers to monitor access or sample loaded files for changes.

Opportunities to Disrupt

Realize that attackers may be able to develop additional attack approaches as they have learned a system and may have stolen information that allows for the development of more powerful future attacks. Defenders should examine their detection and response capabilities. Decision makers should review their restoration plans for attacks with the potential to go deeper into the ICS and could result in damaged equipment. Identify new connections leaving the environment and previously unseen encrypted communications. Network Security Monitoring (NSM) is a great active defense method of detecting exfiltration and ending an adversary's attack path before it disrupts the ICS.

VPN Access

Ukraine Attack

Mitigation guidance based on the attacker approach used in this campaign recommends using two-factor authentication with user tokens to strengthen authentication.

The Next Attack

Attackers may begin looking for existing point-to-point VPN implementations at trusted third party networks or through remote support employee connections where split tunneling is enabled. The immediate mitigation recommendation is to implement trusted jump host or intermediary systems with Network Access Control (NAC) enforcement. Additionally, a VPN configuration approach that disables split tunneling should be enforced.

Opportunities to Disrupt: Defenders are reminded that having remote access through a trusted connection is advantageous for an attacker. Begin by asking why each trusted communication path exists, evaluate the risk, and eliminate each path that does not have an identified need that outweighs the risk of having an attack path. For those communication paths that must remain, consider implementing time of use access for users. Implement the ability to disconnect these paths in an automated way after a defined period of time after access in granted, and a method to disconnect manually if needed. From a passive defense perspective, force choke points in the environment by ensuring that the remote VPNs enter into the environment through a dedicated remote access DMZ. This ensures that traffic and connections can be monitored by active defenders using techniques such as network security monitoring to identify abnormalities in duration of connections, number of connections, and time the connections occur.

Workstation Remote Access

Ukraine Attack

Based on the details provided, the adversaries used the organizations' workstations remotely (while the attacker was physically remote, logically they were local to the host) to conduct Stage 2 of the attack. Mitigation recommendations focus on disabling remote access at the host and at the perimeter firewall.

The Next Attack

Adversaries may modify attack approaches to load additional remote access tools, utilize remote shell capabilities, and tunnel communications over authorized perimeter firewall communications. In response to this modified attack approach, mitigation efforts should focus on host based application aware firewalls, application whitelisting, and configuration management efforts to identify changes in the operation of an asset. Application whitelisting, if installed on the operator HMI to prevent installation of unauthorized remote access software, will not aid in the prevention of authorized software. Also, keep in mind that specific control system vendors may not approve of the whitelisting software.

Opportunities to Disrupt

As a defender prepares for a cyber asset within a trusted environment that may be compromised and remotely controlled, they must consider approaches to quickly move to a conservative operations environment where the ability to issue control signals from untrusted assets is paused. Proper architecture would dictate the ability to segment or disable activities such as remote connections, and unnecessary outbound communications, while conducting active defense mechanisms; such as incident response prior to restoring operational control capabilities to known good assets.

Control and Operate

Ukraine Attack

As the attackers utilized the operator HMI's, they operated numerous sites under the control of the dispatcher. Mitigation approaches for this specific action would focus on application level logic requiring confirmation from the operator, or implement Area of Responsibility (AoR) limitations that only allow an operator to effect certain components of a system. For example: If an entity implemented AoR on one operator workstation that provided east breaker control, and a second operator workstation that provided West breaker control, then an adversary positioned on one workstation would be limited to the AoR allowed on that specific workstation. Some vendor systems allow for Username determined AoR, Workstation determined AoR, and/or an intersection model that combines username and workstation identifier in AoR authorization. There are variations amongst vendor systems in how authentication is handled within the local workstation, directory, or at the application.

The Next Attack

When an attacker identifies a workstation with application security controls in place that limits their capabilities, they may modify their attack to control the system directly by issuing or injecting control commands. Mitigation strategies for this approach would focus on communication path authentication or protocol authentication that would require commands to be issued from an authorized asset. Monitoring communication sessions between hosts can lead to early detection and investigation of suspicious communications.

Opportunities to Disrupt

Preparing for adversarial utilization of cyber assets, or communication paths to control and operate elements of an ICS system, requires system defenders to develop a response approach that eliminates entire sections of cyber asset elements and networks in an effort to inhibit automated control and activate manual operations only. As adversaries learn the environment, they may issue test commands and interact with the SCADA environment without the intention to disrupt it. For mitigation purposes, defenders must talk to operators and ask about abnormal occurrences, and from a passive defense perspective, ensure that logs are collected not only from the host but also from the SCADA applications. Additionally, implement a log aggregation architecture that replicates log files from assets into a log correlation system. Finally, have active defenders routinely review these logs in conjunction with other monitoring activity throughout the ICS to identify abnormalities.

Tools and Technology impacts

Ukraine Attack

The attackers used multiple approaches to impact communication tools, operator technology for restoration efforts, and facility infrastructure essential to many operator activities. Therefore, mitigation recommendations are varied. Items to focus on are:

- Establishing filtering and response capabilities at telecom providers to activate during an ongoing TDoS attack
- Disable remote management of field devices when they are not required.
- Disconnect building control infrastructure systems from the ICS network.
- Consider the number of spares required for embedded systems to regain required communication or control/protection.

The Next Attack

A subsequent attack may progress from resource consumption to a more direct communication path outage that affects communication capabilities. To mitigate this approach, defenders need to establish alternate communications infrastructure for essential service capabilities.

After an attacker identifies increased security requirements for field device management, they may attempt to establish direct access to a field device through a local asset with connectivity or physical presence at the site for direct firmware manipulation. Mitigation strategies for this attack approach focus on electronic and physical access controls and the development of a rapid response capability during an attack or incident.

Opportunities to Disrupt

A determined adversary can impact remote assets either electronically or physically. A defender should develop strong recovery and restoration approaches to replace mission-critical cyber asset components. One option is to rely on inventory and mutual aid assistance from trusted peer organizations and/or suppliers. In cases where specific assets are not immediately recoverable, it is necessary to develop the ability to operate the larger system with operational islands that can be recovered in a timely manner.

Defenders should have access to and visibility of the ICSs to be able to identify abnormal behavior around field device interaction. For example, uploading firmware outside of a scheduled downtime should be quickly observable. Firmware modifications over the network cause spikes in network traffic that active defenders should be consistently looking for. See Figure 10 for an example of a malicious firmware update to an industrial network switch. Even without knowing the baseline of normal activity, which defenders should have, it can be trivial to spot firmware updates in network data.

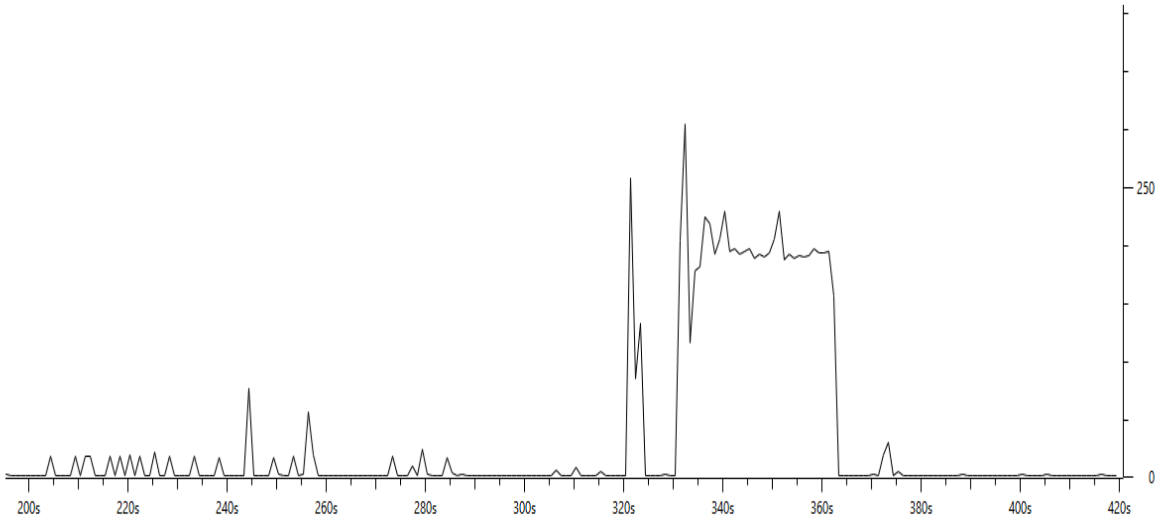


Figure 10: Sample Network I/O Data from a Malicious Firmware Update to an Industrial Ethernet Switch[37]

Respond and Restore

Ukraine Attack

The cyber attacks performed against three Ukrainian oblenergos were well planned and highly coordinated. The attacks consisted of several major elements with both enabling and supporting attack segments. The attackers were remote and interacted with multiple locations within each of their targets to include central and regional facilities. Distribution utilities traditionally have both central business and engineering office(s) and a number of branch facilities used to support line crew, meter reading, bill payment, and distributed supervisory control operations. Certain types of cyber attacks designed to maliciously take over and operate a SCADA DMS may be best performed in a distributed fashion at the lowest or most direct level (from a local dispatch and SCADA server out to the substations that are being monitored and controlled). Preparing for a high-tempo, multifaceted attack is not easy and it requires careful plan review, testing, integrated defense, and operations exercises. Rehearsing steps to more quickly sever or prevent remote access, to safely separate the ICSs from connected networks, or to contain and isolate suspicious hosts is critical.

The Next Attack

The next attack may purposefully differ in its approach to throw off or defeat the defender's plans and expectations. It is critical that defenders exercise and train against different scenarios and be aware that attackers are co-adaptive and creative. It is vital to develop capabilities with flexibility in mind.

Opportunities to Disrupt/Restore

Operations personnel must be involved in planning for restoration from a successful Stage 2 ICS attack. Concepts to consider from an electric operations and engineering perspective include the following and are graphically depicted in Figure 11:

- Cyber contingency analysis: Continuous analysis and preparing the system for the next event.
- Cyber failure planning: Modeling and testing cyber system response to network and asset outages.
- Cyber conservative operations: Intentionally eliminating planned and unplanned changes as well as stopping any potentially impactful processes.

[37] For a good discussion on exploits and malicious firmware updates for industrial ethernet switches see the research by Eireann Leverett, Colin Cassidy, and Robert M. Lee in the DEFCON presentation "Switches Get Stitches" here: https://www.youtube.com/watch?v=yaY3rtA37Uc

- Cyber load shed: Eliminating unnecessary network segments, communications, and cyber assets that are not operationally necessary.
- Cyber Root Cause Analysis (RCA) : RCA forensics to determine how an impactful event occurred and ensure it is contained.
- Cyber Blackstart: Cyber asset base configurations and bare metal build capability to restore the cyber system to a critical service state.
- Cyber mutual aid: Ability to utilize information sharing and analysis centers (ISACs), peer utilities, law enforcement and intelligence agencies, as well as contractors and vendors to respond to large-scale events.

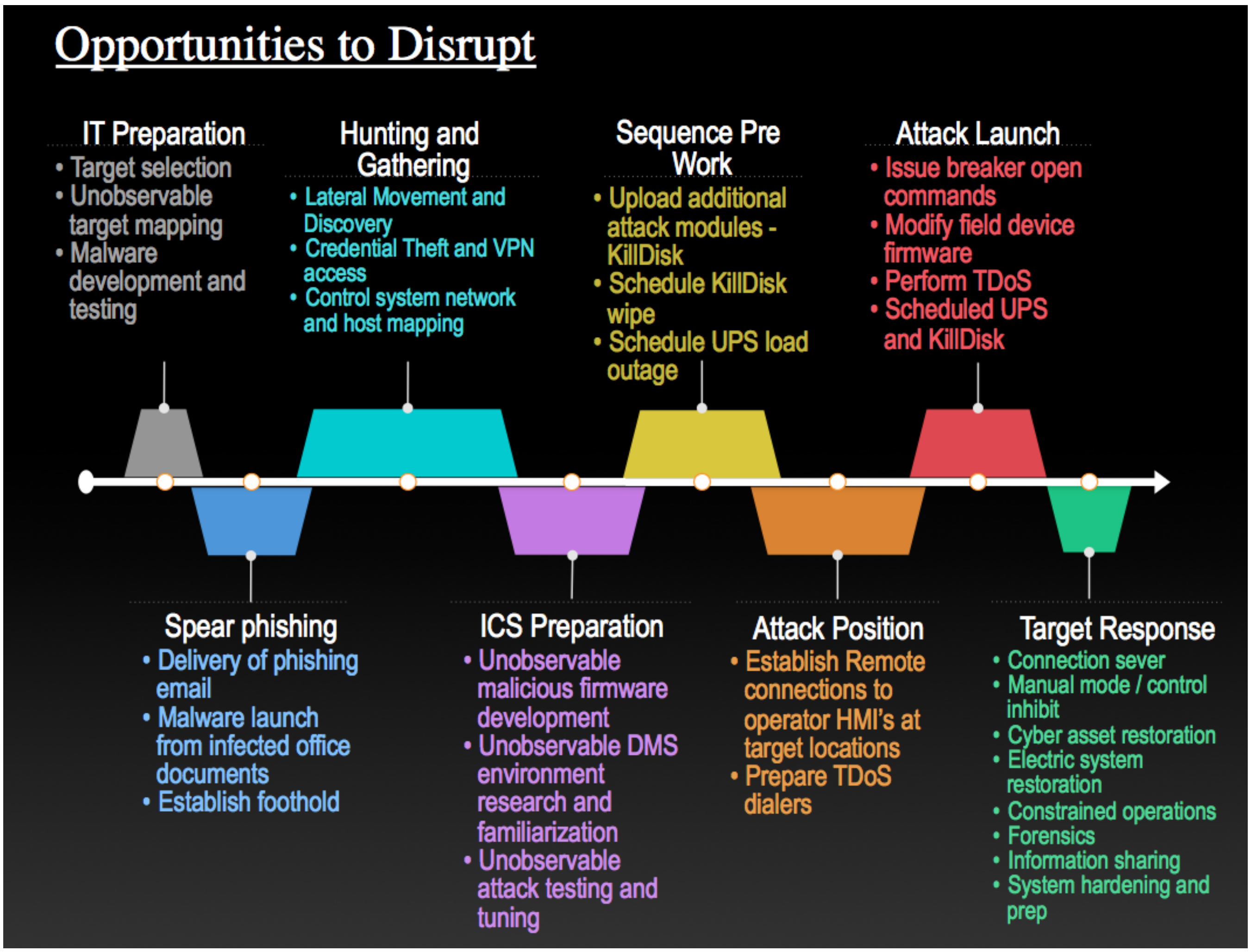


Figure 11: Summary of the opportunities to disrupt the attack

Recommendations

Architecture

Recommendations:

- Properly segment networks from each other.
- Ensure logging is enabled on devices that support it, including both IT and Operational Technology (OT) assets.
- Ensure that network architecture, such as switches, are managed and have the ability to capture data from the environment to support Passive and Active Defense mechanisms.
- Make backups of critical software installers and include an MD5 and SHA256 digital hash of the installers.
- Collect and vault backup project files from the network.
- Test the tools and technologies that passive and active defense mechanisms will need (such as digital imaging software) on the environment to ensure that it will not negatively impact systems.
- Prioritize and patch known vulnerabilities based on the most critical assets in the organization.
- Limit remote connections only to personnel that need them. When personnel need remote access, ensure that if they do not need control that they do not have access to control elements. Use two-form authentication on the remote connections.
- Consider use of a system event monitoring system, configured and monitored specifically for high-value ICS/SCADA systems.

Passive Defense

Recommendations:

- Application whitelisting can help limit adversary initial infection vectors and should be used when not too invasive to the ICSs.
- DMZs and properly tuned firewalls between network segments will give visibility into the environment and allow defenders the time required to identify intrusions.
- Establish a central logging and data aggregation point to allow forensic evidence to be collected and made available to defenders.
- Implement alarm package priorities for abnormal cyber events within the control system.
- Enforce a password reset policy in the event of a compromise especially for VPNs and administrative accounts.
- Utilize up-to-date antivirus or endpoint security technologies to allow for the denial of known malware.
- Configure an intrusion detection system so that rules can be quickly deployed to search for intruders.

Active Defense

Recommendations:

- Train defenders to hunt for odd communications leaving the networked environment such as new IP communications.

- Perform network security monitoring to continuously search through the networked environment for abnormalities.
- Plan and train to incident response plans that incorporate both the IT and OT network personnel.
- Consider active defense models for security operations such as the active cyber defense cycle.
- Ensure that personnel performing analysis have access to technologies such as sandboxes to quickly analyze incoming phishing emails or odd files and extract indicators of compromise (IOCs) to search for infected systems.
- Use backup and recovery tools to take digital images from a few of the systems in the supervisory environment such as HMIs and data historian systems every 6-12 months. This will allow a baseline of activity to be built and make the images available for scanning with new IOCs such as new YARA rules on emerging threats.
- Train defenders on using tools such as YARA to scan digital images and evidence collected from the environment but do not perform the scans in the production environment itself.

Good architecture and passive defense practices build a defensible ICS; active defense processes establish a defended ICS environment. Countering flexible and persistent human adversaries requires properly trained and equipped human defenders.

Implications and Conclusion

Implications for Defenders

The remote cyber attacks directed against Ukraine's electricity infrastructure were bold and successful. The cyber operation was highly synchronized and the adversary was willing to maliciously operate a SCADA system to cause power outages, followed by destructive attacks to disable SCADA and communications to the field. The destructive element is the first time the world has seen this type of attack against OT systems in a nation's critical infrastructure. This is an escalation from past destructive attacks that impacted general-purpose computers and servers (e.g., Saudi Aramco, RasGas, Sands Casino, and Sony Pictures). Several lines were crossed in the conduct of these attacks as the targets can be described as solely civilian infrastructure. Historic attacks, such as Stuxnet, which included destruction of equipment in the OT environment, could be argued as being surgically targeted against a military target.

Infrastructure defenders must be ready to confront highly targeted and directed attacks that include their own ICSs being used against them, combined with amplifying attacks to deny communication infrastructure and future use of their ICSs. The elements analyzed in the attack indicated that there was a specific sequence to the misuse of the ICSs, including preventing further defender use of the ICSs to restore the system. This means that the attacker "burned the bridges" behind them by destroying equipment and wiping devices to prevent automated recovery of the system. The attacks highlight the need to develop active cyber defenses, capable and well-exercised incident response plans, and resilient operations plans to survive a sophisticated attack and restore the system.

Nothing about the attack in Ukraine was inherently specific to Ukrainian infrastructure. The impact of a similar attack may be different in other nations, but the attack methodology, Tactics, Techniques, and Procedures (TTPs) observed are employable in infrastructures around the world.

Conclusion

We have identified five themes for defenders to focus on as they consider what this attack means for their organization:

Theme 1

As defenders of ICSs, consider the sequence of events taken by the adversary in the months leading up to December 23, 2015 when this cyber operation targeting Ukrainian electricity infrastructure was planned and developed. The operation relied upon intrusions that appear to have come from a broader access campaign conducted in the spring of 2015. In a prolonged attack campaign, there are likely numerous opportunities to detect and defend the targeted system. The two-stage ICS cyber kill chain helps note that in an ICS environment, there is an increased window for the detection and identification of the most concerning attack types.

Theme 2

The cyber attacks were conducted within minutes of each other against three oblenergos, resulting in power outages affecting approximately 225,000 customers for a few hours. While the total number of customers across three service territories does not add up to a significant number of customers or load across Ukraine, there may be significance in target selection or specific loads. One critical element of this particular attack was its coordinated nature affecting three target entities and the thoroughness of the adversary sequence of events in achieving their goals. Important opportunities for defenders to disrupt the adversary's sequence of events were identified.

Theme 3

The cyber attacks were mislabeled as solely linked to BlackEnergy 3 and KillDisk. BlackEnergy 3 was simply a tool

used in Stage 1 of the attacks and KillDisk was an amplifying tool used in Stage 2 of the attacks. BlackEnergy 3 malware was used to gain initial footholds into a multitude of organizations within Ukraine and not just the three impacted oblenergos. It is unknown if the adversary had planned to use this access campaign to enable their operation or if achieving access was the motivation leading to the development of a concept to attack the power system.

Excessive focus on the specific malware used in this attack places defenders into a mindset in which they are simply waiting for guidance on the specific attack components so they can eliminate them. This attack could have been enabled by a variety of approaches to gain access and utilize existing assets within a target environment. Regardless of the initial attack vector, the ICS tools and environment were ultimately used to achieve the desired effect, not the BlackEnergy 3 malware.

Theme 4

The attack concept had to be able to work across multiple SCADA DMS implementations and target common susceptible elements, such as storage overwrites for Windows-based operating system workstations and servers. The attackers likely developed destructive firmware overwrite techniques after discovering accessible embedded systems. There was likely a significant amount of unobservable adversarial testing performed prior to introducing the attack into the environment. Many capabilities were demonstrated throughout this attack, and they all provide specific lessons learned for defenders to take action on.

Theme 5

Information sharing is key in the identification of a coordinated attack and directing appropriate response actions. Within the Ukraine, an organization with the ability to enable appropriate information sharing and provide incident response guidance should be pursued. In the United States and other countries with established information sharing mechanisms, such as ISACs (Information Sharing and Analysis Centers), the focus should be on maintaining and improving the information provided by asset owners and operators. This increased data sharing will enhance situation awareness within the sector, which will in turn lead to earlier attack detection and facilitate incident response.

In many ways, the Ukrainian oblenergos and their staff, as well as the involved Ukrainian government members deserve congratulations. This attack was a world first in many ways, and the Ukrainian response was impressive with all aspects considered.

As the investigation and analysis of technical data continues and more information regarding this attack surfaces, the authors of this DUC will update this report where appropriate in an effort to maintain the most accurate and beneficial guidance document possible for ICS defenders. The E-ISAC will continue to provide credible reporting and guidance as well.

Appendix Information Evaluation

Credibility: 5[38]

The claims by the Ukrainian government that outages in the service territory of the targeted electricity companies were caused by a series of cyber attacks have been confirmed. The claim was originally met with private skepticism by the SANS ICS team as ICS organizations frequently have reliability issues and incorrectly blame cyber mechanisms such as malware found on the network that is unrelated to the outage. Early reporting on incidents is often rushed and stressful which leads to inaccurate claims. However, in the Ukrainian case, there is a large amount of evidence available; including malware samples, interviews with operators present during the incident, and confirmation by multiple private companies involved in the incident. Lastly, the U.S. government has since also confirmed the attacks due to their own investigation.

The most recent report released from DHS ICS-CERT[39] cites direct interviews with "operations and information technology staff and leadership at six Ukrainian organizations with first-hand experience of the event." Based on the information provided in the report,[40] the U.S. delegation interviewed and considered information from the three impacted organizations as well as others. The format of the interviews, and asset owner and operator discussions, indicated that "the team was not able to independently review technical evidence of the cyber-attack. However, a significant number of independent reports from the team's interviews as well as documentary findings corroborate the events…".[41] However, a large amount of technical information was made available to the larger community including indicators of compromise, malware samples, technical information about the ICS itself and its components, and some samples of logs from the SCADA environment.[42] The majority of sources to date have relied upon initial attempts by Ukrainian power entities to inform customers about the cause of the outage and sources derived from interviews with impacted entities. The DHS report does not attempt to assign attacker attribution and neither will this DUC.

Amount of Technical Information Available: 4[43]

A score of 4 has been assigned for the technical information available due to the fact that malware samples, observable ICS impacts, technical indicators of compromise, and first hand interviews were available. The investigation also included a joint working group between the Ukrainian government, impacted oblenergos, and U.S. government representatives starting on January 18, 2016.[44] This amount of information was sufficient to confirm the attacks.

However, it should be noted that there may be pieces of information missing due to the lack of visibility in various parts of the ICS network. As an example, packet captures from the network during the attack and field

---

[38] Credibility of the information is rated in a scale from [0] Cannot be determined, [1] Improbable, [2] Doubtful, [3] Possibly true, [4] Probably true, [5] Confirmed

[39] https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

[40] SANS ICS team members have been able to view technical data in both public and non-government private channels to confirm the existence of forensic data and the core components of the analysis based off of the data.

[41] https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

[42] It should be noted that many in the community would like access to internal forensic logs of the impacted oblenergos. This is an understandable request but it is extremely rare for impacted organizations to make such information publicly available. SANS ICS team members have been able to view technical data in both public and non-government private channels to confirm the existence of forensic data and the core components of the analysis based off of the data.

[43] Amount of Technical Information Available is an analyst's evaluation and description of the details available to deconstruct the attack provided with a rating scale from [0] No specifics, [1] high-level summary only, [2] Some details, [3] Many details, [4] Extensive details, [5] Comprehensive details with supporting evidence

[44] http://mpe.kmu.gov.ua/minugol/control/uk/publish/article;jsessionid=CE1C739AA046FF6BA00FE8E8A4D857F3.app1?art_id=245086886&cat_id=35109

device logging were not available. With this information even more about the technical minutia of the attack would be available. The amount of information available as well as the willingness by the impacted oblenergos and Ukrainian government to share that information publicly was the most seen to date for a confirmed intentional cyber attack that impacted the operations of an ICS.

When considering the technical information provided, the authors of this DUC have considered the larger public reporting of electricity customer outages within Ukraine as a component of the validation and evidence necessary to demonstrate the attacker effects to the electricity system. The official public alert by DHS corroborates prior reporting and is based on interviews and information exchanged with the impacted organizations.